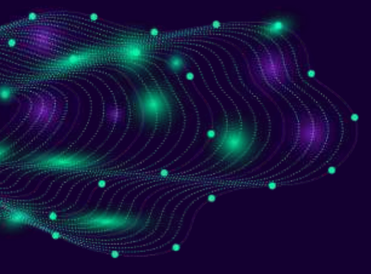
C. Nappi

Mirium

Cyber Security

Il Valore della Sicurezza

casi reali e suggerimenti pratici



warapn
innovation enabler

Cesare Nappi
CTO Mirium srl

ENABLE X 2024
innovate for excellence

C. Nappi

Sicurezza Informatica

protezione

- **Sistemi Informativi (hardware, software e infrastrutture associate)**
- **Dati, Identità e Servizi**

da

- **accessi non autorizzati**
- **danni o usi impropri (intenzionali o accidentali)**
- **Mancato rispetto di procedure e controlli di sicurezza**

Attacchi o Incidenti?

il 50% degli attacchi avviene sfruttando vulnerabilità *(fonte Kev di Cybersecurity Infrastructure and Security Agency)*

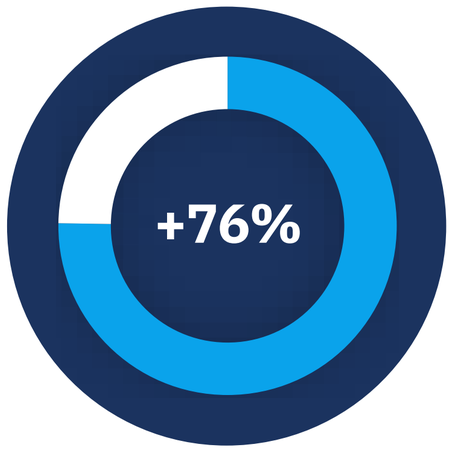
il 49% degli incidenti parte da un azione umana interna (con o senza dolo) *(fonte 2024 Data Breach Investigations Report)*

C. Nappi

Fonte: Rapporto Clusit 2024

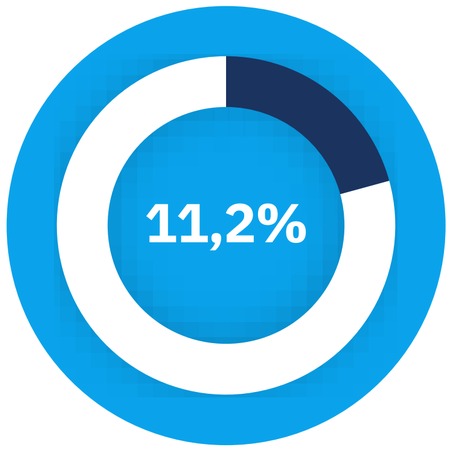
Dati: attacchi in Italia

2018-2023



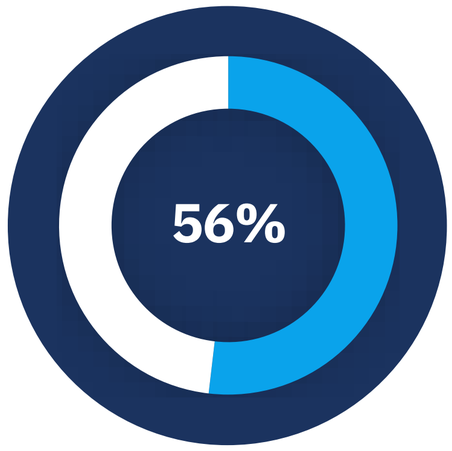
Negli ultimi 5 anni gli attacchi sono cresciuti del 76%

2023



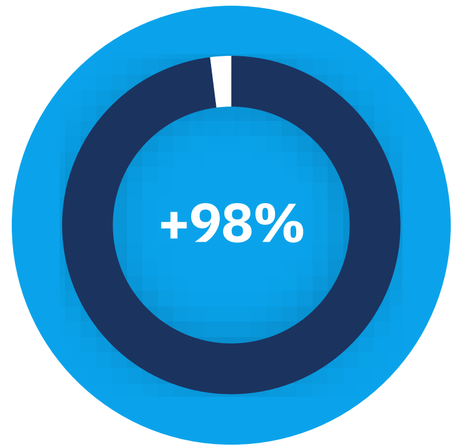
In Italia nel 2023 11,2% degli attacchi globali gravi riusciti

2023



Il 56% degli attacchi è di gravità critica/elevata

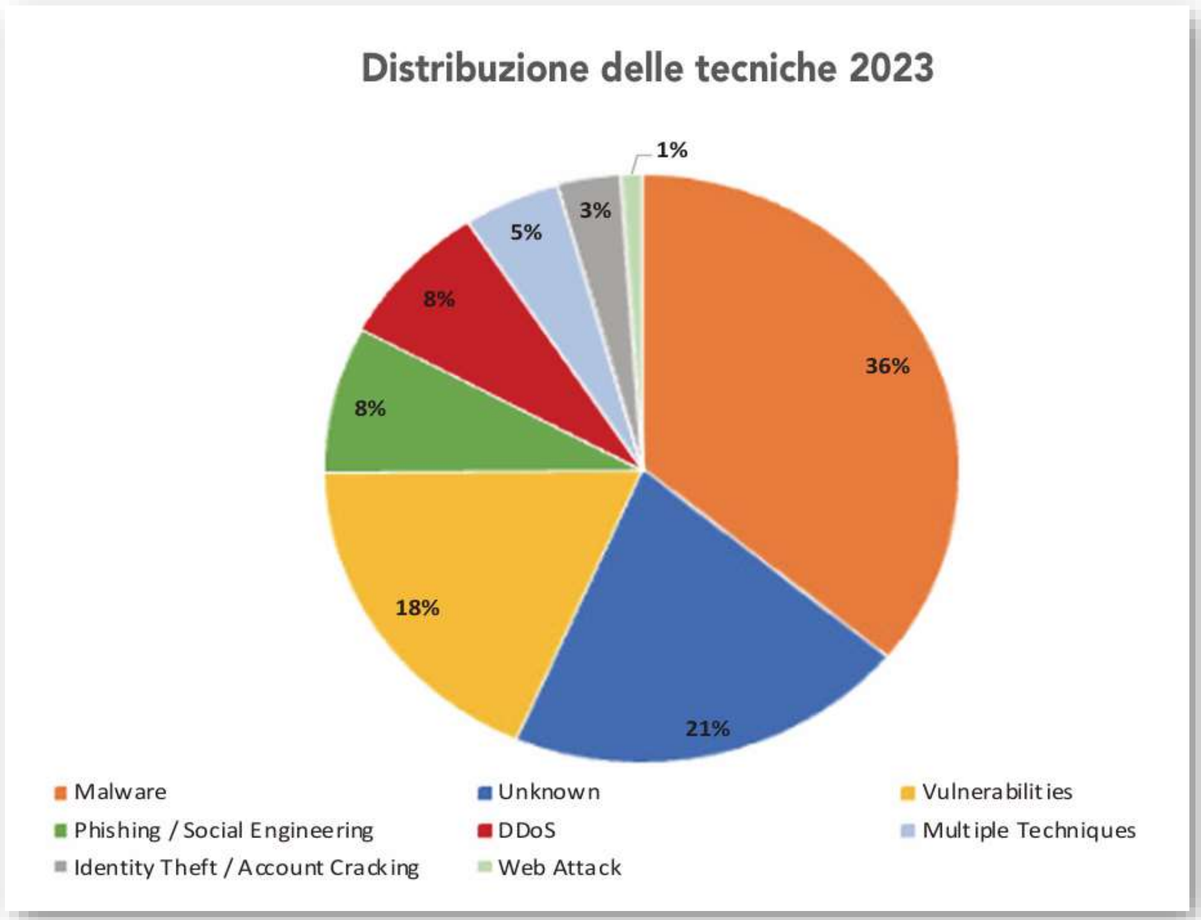
2022-2023

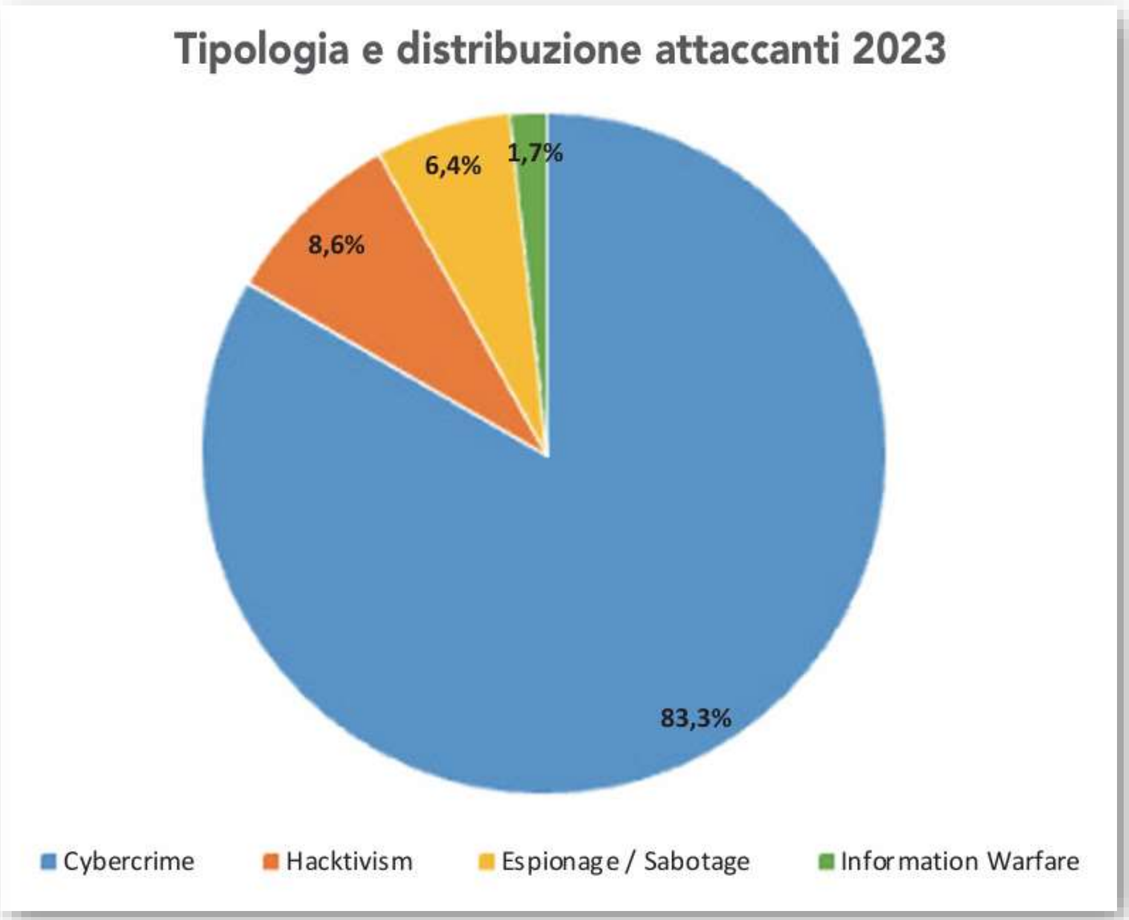


+98% attacchi di tipo DDOS nel 2023 rispetto al 2022

Fonte: Rapporto Clusit 2024

Dati: come e perchè?





C. Nappi

MiriuM

Focus Malware

OBIETTIVI

Il comune obiettivo è ottenere accesso a dati e sistemi, in genere a scopo di estorsione

Malware

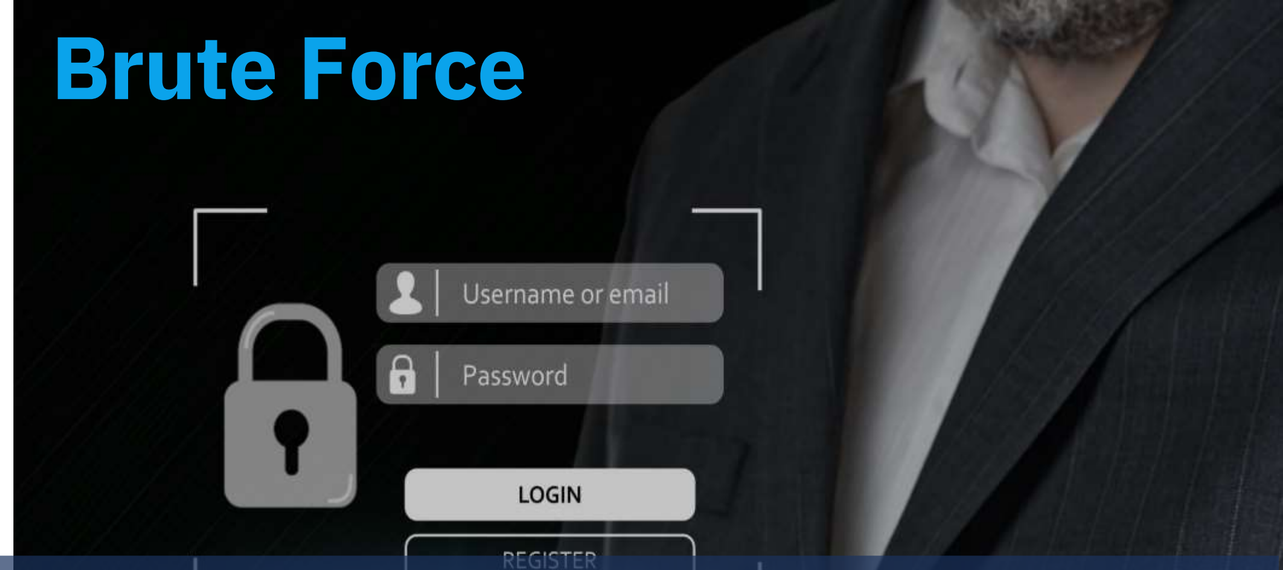
Software dannoso sviluppato ad hoc (anche da IA).

Può essere venduto «pronto all'uso» su piattaforme SaaS (ad es. fenomemo Ransomware As A Service)

Vettori: phishing, siti compromessi, download

Potrebbe non essere individuato se si tratta di uno zero-day o un rootkit

Brute Force



Brute Force

Attacco di forza bruta che avviene «per tentativi» con inserimento di combinazioni multiple di credenziali di accesso sfruttando la debolezza delle password

Talvolta l'insieme delle credenziali viene recuperato da archivi presenti nel Dark Web o acquisiti illecitamente da precedenti data breach

Contromisure: tecniche

C. Nappi

Mirium

Quanto costa un attacco?

Gartner prevede che entro il 2025 il 75% delle aziende subirà un attacco

La Cyber Security rientra a pieno titolo tra i fattori che incidono sulla Continuità Operativa (BC)

Pagare o no?

- Ci si interfaccia con criminali
- Si potrebbe essere attaccati nuovamente
- Non si ha certezza della soluzione
- Si alimenta economia criminale
- Nessuna certezza su pubblicazione dati

Ransomware

Costo del riscatto. Il costo medio di un riscatto in Italia è di 700.000$ *(fonte: Sophos)*

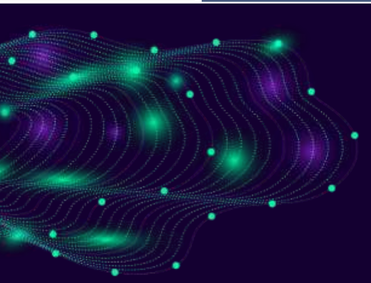
Costo del downtime. Il ripristino completo della operatività aziendale è in media pari a 22 giorni *(fonte: Netapp)*

Sanzioni. Per mancata applicazione delle best practices di protezione dati, data breach GDPR (2% del fatturato), NIS2 (1,4%)

Danno reputazionale. Danno di immagine reputazionale incalcolabile: ridotta fiducia dei clienti e fornitori

DDoS

Costo di interruzione del servizio. Downtime del servizio e QoS compromessa. Grave in caso di servizi critici



warlpn
innovation enabler

Cesare Nappi
CTO Mirium srl

ENABLE X 2024
innovate for excellence

Attività di consulenza

Caso reale: vulnearbility assessment

Cliente: fatturato ~35Mln €
Attività: Assessment ICT
Criticità riscontrate: multiple

Proposta mitigazione
Valore investimento: ~ 12K€

Livello	Criticità/Oggetto	Descrizione
Alto	*Criticità multiple su Dell Power Edge [192.168[redacted]]*	Sul server risulta installato ambiente di virtualizzazione vmware esxi nella versione 5.5, non più supportata e aggiornata dal produttore dal 19/09/2018. La versione risulta vulnerabile a: esecuzione di codice malevolo e privilege escalation (cfr report di dettaglio allegato) L'ambiente virtualizzato ospita a sua volta 2 server virtuali critici [redacted] per ruoli svolti: rispettivamente file server controller di dominio
Alto	*Criticità multiple su server virtuale [redacted] con ruolo di controller di dominio [192.168[redacted]]*	Il server che svolge il ruolo di controller di dominio è dotato di Sistema Operativo Windows Server 2003 non più supportato da Microsoft dal 14/07/2015, pertanto non riceve più aggiornamenti e patch di sicurezza, oltre ad essere obsoleto per i sistemi operativi dei client che gestisce Il ruolo è vitale per tutte le operazioni di AAA (Autenticazione, Atuorizzazione e Accounting), al punto che nella configurazione tipica esiste un controller di dominio secondario che ne svolge le veci in caso di fault del primario. Non esiste controller di dominio secondario. Sul server è installato anche un database firebird sql configurato con le credenziali di default ed esposto sulla porta 3050 Il server è vulnerabile anche a "SMB Server Multiple Vulnerabilities-Remote" che consente di eseguire codice da remoto ed esfiltrare informazioni (cfr. report allegato di dettaglio)
Alto	*Criticità multiple su server virtuale [redacted] con ruolo di file server [192.168[redacted]]*	La versione del web server IIS installata è vulnerabile alla esecuzione di codice da remoto e non è stata aggiornata Sul server è installato anche un database firebird sql configurato con le credenziali di default ed esposto sulla porta 3050

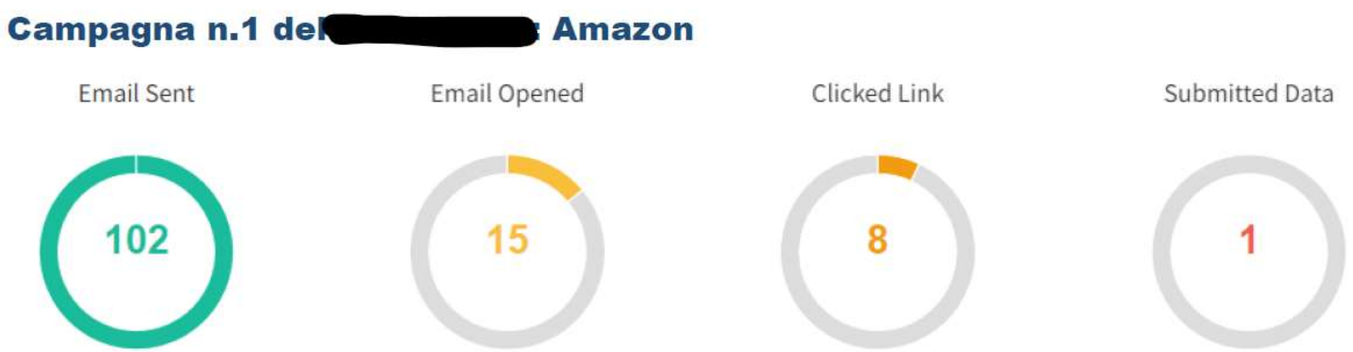
Conseguenze: ~ Attacco ransomware gruppo Lockbit a tre mesi dal report assessment
Vettore e metodo: e-mail phishing, pc infetto, deploy script malevolo su DC 2003
Fermo attività: totale per 7gg - ripristino completo dopo 40gg

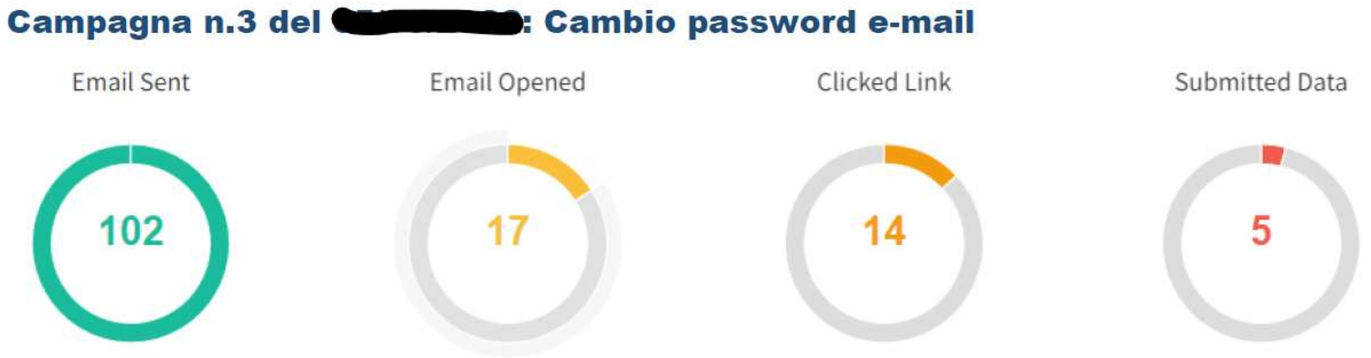
Attività di consulenza

Caso reale: phishing simulation

Cliente: fatturato ~4Mln €
Attività: Phishing Simulation

Campagne sottoposte: 3
E-mail Aperte: 16%
Click su link: 10%
Invio dati: 3%

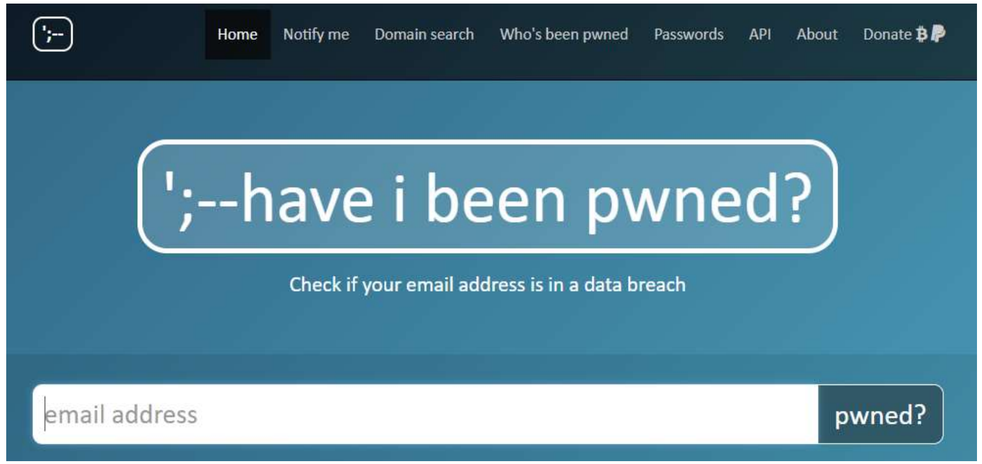


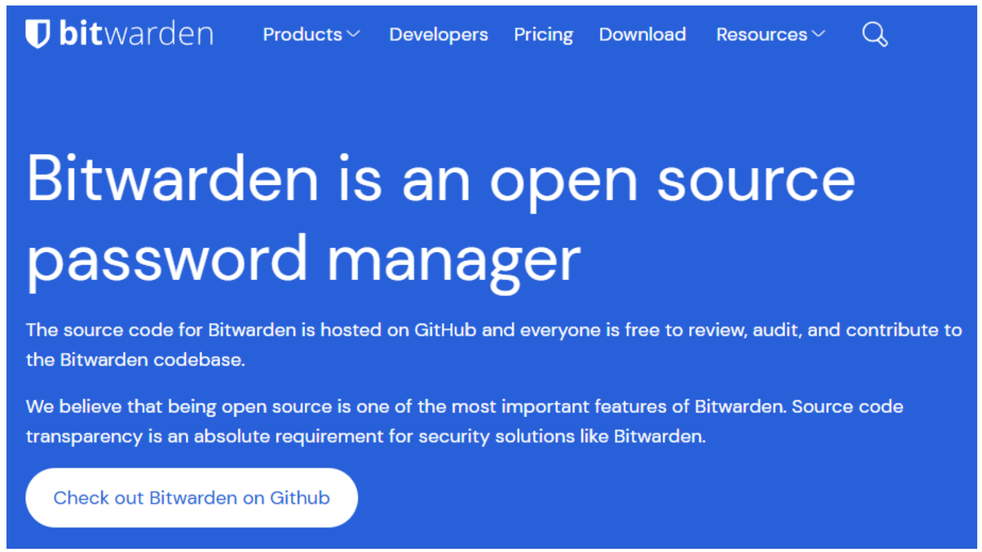


Esiti: Avvio attività formativa sulla consapevolezza dei rischi e distribuzione materiale formativo

Strumenti pratici Password

HTTPS://HAVEIBEENPWNED.COM/





TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2024

How did we make this? Learn at hivesystems.com/password

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	3 secs	6 secs	9 secs
5	Instantly	4 secs	2 mins	6 mins	10 mins
6	Instantly	2 mins	2 hours	6 hours	12 hours
7	4 secs	50 mins	4 days	2 weeks	1 month
8	37 secs	22 hours	8 months	3 years	7 years
9	6 mins	3 weeks	33 years	161 years	479 years
10	1 hour	2 years	1k years	9k years	33k years
11	10 hours	44 years	89k years	618k years	2m years
12	4 days	1k years	4m years	38m years	164m years
13	1 month	29k years	241m years	2bn years	11bn years
14	1 year	766k years	12bn years	147bn years	805bn years
15	12 years	19m years	652bn years	9tn years	56tn years
16	119 years	517m years	33tn years	566tn years	3qd years
17	1k years	13bn years	1qd years	35qd years	276qd years
18	11k years	350bn years	91qd years	2qn years	19qn years

HIVE SYSTEMS

› Hardware: 12 x RTX 4090 | Password hash: bcrypt

Password personale di un servizio: 8wDkZY7FW3%mUFKJ=!tZF2

Strumenti pratici Crittografia e Backup

Abilitare i servizi nativi di crittografia o utilizzare tool di terze parti

- GDPR compliant
- Utile in caso di furto dispositivo o data breach

Smartphone
- Android
- Apple

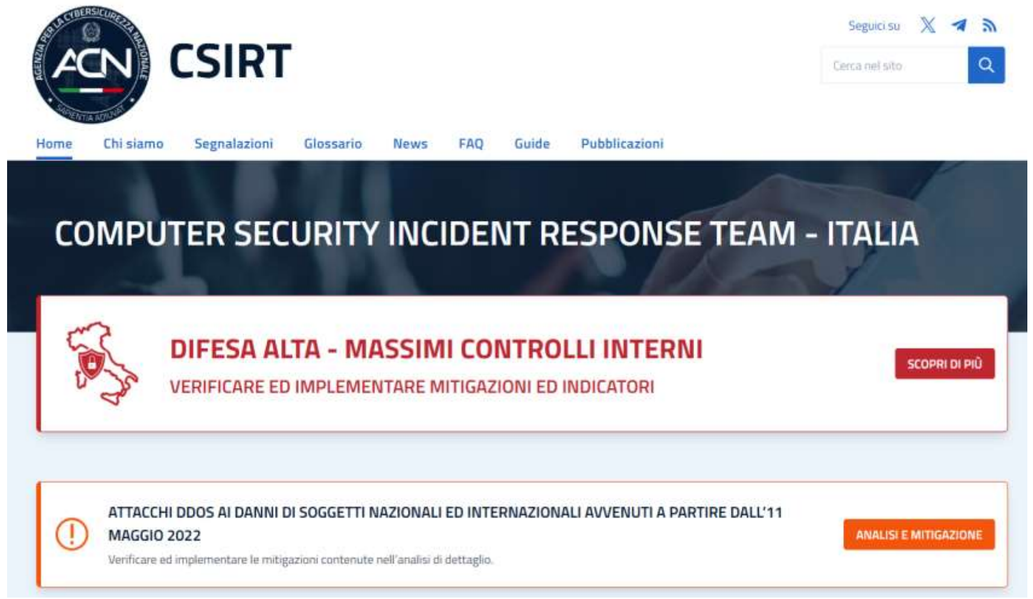
PC/Laptop
- Bitlocker
- File Vault

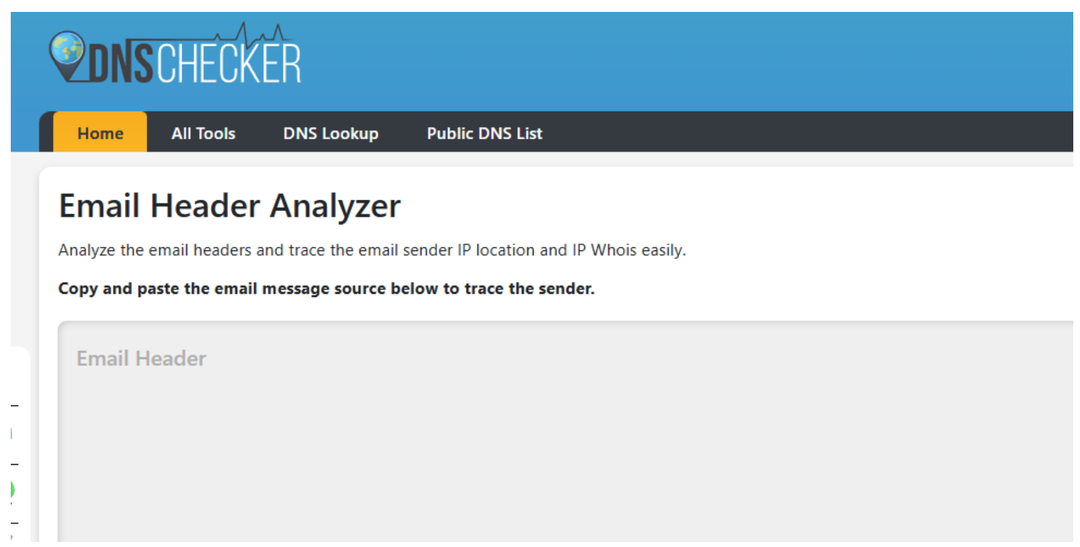
Servizi Cloud
- Google
- i-Cloud
- Microsoft 365

Regola backup 3-2-1

- 3 copie dei dati
- su almeno 2 destinazioni differenti
- almeno 1 offsite

Strumenti pratici Siti utili





C. Nappi

Cesare Nappi
CTO Mirium srl

innovation enabler

ENABLE X 2024
innovate for excellence

Strumenti pratici VPN e DNS

C. Nappi

RISCHI DI CONNESSIONE A RETI PUBBLICHE (WI-FI, ETC)

- Attacchi MITM (Man In The Middle)
- Furto di identità e dati personali (traffico in chiaro)
- Sniffing del traffico
- Re-indirizzamento a siti malevoli

VPN - SDWAN - ZTNA

STABILIRE UNA CONNESSIONE «SICURA» (TUNNELING)

- Remote Working o Navigazione Pubblica
- Tutela della Privacy: l'IP di navigazione è un dato personale
- Principio del minimo privilegio (ZTNA)
- Superamento di restrizioni di traffico

FILTRO DNS

FILTRO A MONTE SUL TRAFFICO

- Semplice da impostare
- Rispetto della Privacy (DNS over HTTPS)

DNS0.EU | quad9

C. Nappi

Sicurezza Umanocentrica

Misure Tecniche

Sistemi di Protezione (Firewall, IDS, IPS)

Password complesse e MFA, ZTN

Crittografia dati

Backup e repliche off site

Patching

Misure Organizzative

Piano Disaster Recovery

Business Continuity

Cybersecurity Awareness (formazione)

Phishing Simulation

Incident Response

Progetto

Valore Compliance

Crescita in solidità, reputazione e valore

C. Nappi
Mirium

“CHI NON PROGETTA LA SICUREZZA PROGRAMMA IL FALLIMENTO.”

KEVIN MITNICK – (2002, THE ART OF DECEPTION)

Grazie

MiriuM
SOLUZIONI INNOVATIVE

È solo il nostro sito, ma attenzione: potrebbe essere «Quishing» !